UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,652	06/19/2000	THOMAS A BERSON	XER1P002	4307

7590 07/06/2005

Patent Documentation Center
Xerox Corporation
100 Clinton Avenues., Xerox Sq. 20th floor
Rochester, NY 14644

EXAMINER	
GURSHMAN, GRIGORY	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/596,652	BERSON ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-15 and 17-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-15 and 17-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/01/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's amendment of the independent claims 1, 13 and 20, reflects issues necessitating the new grounds of rejection provided herein. Accordingly, Applicant's arguments and remarks based on claims as currently amended have been thoroughly considered, but are mute in view of the new grounds of rejections.

2. The rejections of claims 1-3, 5-15 and 17-22 are provided herein.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The claimed invention of claim 20 is directed to non-statutory subject matter. A system comprising various logics is non-statutory per se, because the system is not recited as a computer system and the logic is not recited as executable on the computer or computer implemented system.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-15 and 17-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGravey (U.S. Patent No. 6.643.774 B1) in view of Dolan (U.S. Patent No. 5.604.801).

5. Referring to the instant claims, McGravey discloses a method for delegating authority in a public key authentication environment from a client to a server machine or process, in order that the server machine or process can then securely access resources and securely perform tasks on behalf of the client (see abstract). McGravey shows in Fig. 6 that the client sends an initial request at 601, comprising a nonce (nonce1) and a request for the server's certificate. The server forwards or tunnels all the client information received from the client during the handshaking process on to the private key system as shown at 602. The private key system now has the nonce1 (from the client), and the original request from the client. The private key system responds 603 by sending a signed nonce1, a nonce2, and the private key system's certificate (identified in FIG. 6 as the security certificate) to the server. The server then forwards 604 this information to the client. The client then responds 605 by sending a signed nonce2 and the client certificate to the server. The server forwards 606 or tunnels this information to the private key system.

6. Referring to the independent claims 1, 13 and 20, the limitation "identifying a client utilizing the network" is met by the client, which sends an initial request at 601, comprising a nonce (nonce1) and a request for the server's certificate (see Fig.6).

The limitation "receiving information at the server from the client ... wherein the information is encrypted by the client using the first key and performing cryptographic service at the server" is met by the private key system (i.e. client connected to the server) sending a signed nonce1, a nonce2, and the private key system's certificate (identified in FIG. 6 as the security certificate) to the server. The limitation "server off-loads a computation burden associated with the cryptographic service from the client" is met by teaching of McGravey that the server tunnels all the client information on to the private key system as shown at 602, thereby generating atunnel on the network and off-loading the cryptographic service from the client. McGravey, however does not explicitly teach receiving the encrypted client's private key at the server and performing the cryptographic service by the server using the decrypted client's private key of a public key pair.

7. Referring to the instant claims, Dolan discloses a public key communication system (see Fig. 1). Dolan teaches a data communications system is described in which messages are processed using public key cryptography with a private key unique to one or more users (150). The server (130) has access to, the private key for each, user in encrypted form only. The private key is encrypted with a key encrypting key and each security device (120) comprises means for storing or generating the key encrypting key and providing the key encrypting key to the server (130). The server comprises secure means (360) to retrieve the encrypted private key for the user, decrypt the private key using the key encrypting key, perform the public key processing using the decrypted private key.

8. Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to receive information at the server from the client over the tunnel of McGravey and perform the public key processing (i.e. cryptographic service) using the decrypted private key of the client as taught in Dolan. One of ordinary skill in the art would have been motivated to receive encrypted client's private key at the server from the client over the tunnel of McGravey and perform the cryptographic service using the decrypted private key of the client as taught in Dolan for generation of digital signatures (see Dolan, column 1, lines 7- 10).

9. Referring to claims 3, 15 and 21, McGravey teaches sending a signed nonce1, a nonce2 (see Fig.6), which meets the limitation "key comprises at least one parameter for the cryptographic service performed by the server".

10. Referring to claims 5, it is well known in the art to perform modular exponentiation at the server. One of ordinary skill in the art would have been motivated to perform modular exponentiation at the server in order not to reveal the client secret to the server.

11. Referring to claims 6 and 18, "transmitting the cryptographic service result to the client" is met by the server, which sends 610 the session credential and a request for the ticket(s) to the private key system (see McGravey, Fig.6).

12. Referring to claim 22, it is well know in the art to have the message blinded by the user before transmittal to the server. One of ordinary skill in the art would have been motivated to have the message blinded prior to transmission for added security in case of interception.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG
January 7, 2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100